UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/673,422	12/07/2000	Hideaki Takechi	MTS-3221US	8670

7590	04/07/2004

Ratner & Prestia
One Westlakes Berwyn Suite 301
PO Box 980
Valley Forge, PA 19482-0980

EXAMINER
QUINONES, EDEL H

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 04/07/2004

9

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/673,422	TAKECHI ET AL.
	Examiner	Art Unit	
	Edel H Quinones	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on _07 December 2000_.
2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) _1-16_ is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) _1-16_ is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.
10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a) ☒ All   b) ☐ Some * c) ☐ None of:
    1. ☒ Certified copies of the priority documents have been received.
    2. ☐ Certified copies of the priority documents have been received in Application No. _____.
    3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _7_.
4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____ .

III. Detailed Action

1.   Claims 1-16 are presented for examination.

Information Disclosure Statement

2.   The information disclosure statement filed on 3/26/01 complies with the provisions of

MPEP § 609. It has been placed in the application file, and the information referred to therein

has been considered as to the merits.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis

for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3.   Claims 1-5, 7, and 9-16 are rejected under 35 U.S.C. 102(e) as being anticipated by

Sullivan et al. (U.S. Patent 6,069,647 and Sullivan hereinafter).

In regards to claim 1, Sullivan discloses a computer (i.e. single peripheral such as a

DVD) (col. 4, lines 53-56) which comprises a system section (i.e. interface unit) (figure 1, item

110) and a application software section (i.e. programmable unit) (figure 1, item 120), and which

takes in copyright claimed (col. 1, lines 48-51), encrypted data (col. 4, lines 43-47) via a digital

interface (i.e. input unit) (figure 1, item 150) for processing therein, wherein

said system section judges that said application software section is legitimate application

software for the protection of copyright (col. 4, lines 20-34), and

if said application software is a legitimate one, said system section passes a key of said

encrypted data to said application software section (col. 7, lines 15-31).

In regards to claim 2, Sullivan teaches wherein said judgement in said system section is

made by performing authentication between said system section and said application software

section (figure 7c).

In regards to claim 3, Sullivan teaches wherein said judgment in said system section is

made by using a CRL (Certificate Revocation List) listing illegitimate or legitimate application

software (col. 4, lines 7-13).

In regards to claim 4, Sullivan teaches wherein said system section obtains said encrypted

key from an external device (col. 7, lines 41-44), decrypts said encrypted data (col. 5, lines 20-

24), and re-encrypts said decrypted data by using said key or another key (col. 5, lines 36-39).

Sullivan does not teach that the system section obtains the encrypted key as a result of an

authentication with the external device. However, obtaining a key as a result of an

authentication procedure is old and well known in the art as disclosed by Sullivan for the

transferring of a decryption key from the interface unit to the programmable unit (i.e. TSK may

be transferred to the programmable unit in a secure manner after establishing a session key

(SESS) between the interface unit and the programmable unit. SESS may be established using a

well-known zero-knowledge authentication procedure) (col. 7, lines 15-19). Therefore, Sulivan

anticipates obtaining the encrypted key as a result of an authentication with the external device.

In regards to claim 5, Sullivan teaches wherein said system section includes a tamper

verification function (i.e. a function to check whether a program preloaded in programmable unit

has been modified without authorization) (col. 4, lines 28-30), and a tamper code (i.e. digital

signature) is embedded into said application software in said application software section (col. 6,

lines 1-9), and wherein said system section reads said tamper code from said application

software section and, using said tamper verification functions (i.e. hash functions), verifies

whether or not said application software has been tampered with, and if is found that said

application software has been tampered with, said system section reports the result of said

verification (col. 6, lines 62-67).

In regards to claim 7, Sullivan teaches a computer which comprises a system section and

an application software section, and which takes in copyright claimed, encrypted data via a

digital interface for processing therein, as discussed for claim 1 above.

Sullivan also teaches wherein said system section sends said data to said application

section (col. 5, lines 36-44).

Sullivan does not explicitly disclose embedding into said data information concerning

application software residing in said application software section.

However, Sullivan teaches that the system section transmits to the software section

information (i.e. TSK key) concerning application software residing in said application software

section (col. 7, lines 15-20). Sullivan also teaches that a way of transmitting a key is by

embedding it within the digital data contents (col. 7, lines 41-44). Therefore, Sullivan anticipates

embedding into said data information (i.e. TSK key) concerning application software residing in

said application software section

In regards to claim 9, the claim limitation recites a medium holding a program to

substantially implement the method of claims 1, 2, 3, 6, 7 or 8, therefore the same rejection

applies.

In regards to claim 10, the claim limitation recites a program substantially implementing

the method of claims 1, 2, 3, 6, 7 or 8, therefore the same rejection applies.

In regards to claim 11, Sullivan teaches a computer (figure 1) having an operating system

(figure 1, item 110) and an application program (figure 1, item 120), in which the application

program performs a task of providing data to a user (i.e. a player program) (col. 6, line 37), a

method of protecting copyrighted received data comprising the steps of:

a) receiving by the operating system copyrighted data (figure 6b, step s650);

b) authenticating by the operating system the application program (figure 7c);

c) encrypting by the operating system the copyrighted data received in step a) (col. 5,

lines 36-39);

d) providing a decryption key form the operating system to the application program

(figure 6a, step s620), if the application program is authenticated in step b);

e) transmitting the encrypted data of step c) from the operating system to the application

program (col. 5, lines 41-44); and

f) decrypting the encrypted data in the application program using the key provided in step

d) (col. 5, lines 62-66).

In regards to claim 12, Sullivan teaches in which step c) includes decrypting the data

received in step a) using another key before encrypting the data in step c) (col. 5, lines 36-39).

In regards to claim 13, Sullivan teaches that step b) includes

i) generating a digital signature in the application program (figure 3, item 350);

ii) sending the digital signature from the application program to the operating system and

storing the signature in the operating system (figure 7c, item 760); and

iii) authenticating the application program using the signature stored in step ii) (figure 7c,

items 770 and 760).

In regards to claim 14, Sullivan teaches in which step b) includes determining a license

classification of the application program, in which the classification is one of i) display-only

permitted and ii) recording permitted (col. 1, lines 43-51 and col. 9, lines 23-33).

In regards to claim 15, Sullivan teaches that step a) includes receiving at least one of

copyrighted audio data and copyrighted video data (col. 3, lines 12-15).

In regards to claim 16, Sullivan teaches that the programmable unit (i.e. application program section) is an open, re-programmable digital platform such as a computer (col. 5, lines 45-54). Sullivan also teaches that both interface unit (i.e. operating system section) and programmable unit (i.e. application program section) may be incorporated as portions of a single peripheral such as a stand-alone digital versatile disc (DVD) player for example (col. 4, lines 53-56). The Examiner takes Official Notice that controlling allocation and usage of resources of the computer by a computer operating system is old and well known in the art. Therefore, Sullivan anticipates that the operating system controls allocation and usage of resources of the computer.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4.   Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sullivan in view of Togawa (U.S. Patent 6,240,530).

In regards to claim 6, Sullivan teaches a computer (i.e. single peripheral such as a DVD) (col. 4, lines 53-56) which comprises a system section (i.e. interface unit) (figure 1, item 110) and an application software section (i.e. programmable unit) (figure 1, item 120), and which takes in copyright claimed (col. 1, lines 48-51), encrypted data (col. 4, lines 43-47) via a digital interface for processing therein (i.e. input unit) (figure 1, item 150).

Sullivan does not teach that:

- the system section includes a plurality of tamper verification functions,

- that a tamper code and type information is embedded in the software in the application software section,

- that the system section reads the tamper code and type from the application software and based on those values selects the corresponding tamper verification function to use to verify whether the software application has been tampered with.

Togawa discloses a system for computer virus (i.e. tampering) extermination (col. 1, lines 8-16).

Togawa teaches that the system includes a plurality of virus extermination programs. Togawa teaches selecting a virus extermination program to execute based on a virus type detected in the software application (col. 9, lines 20-30). The virus extermination programs and virus type of Togawa are analogous to the tamper verification functions and tamper codes of the instant application.

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Sullivan with the teachings of Togawa to include that the system section includes a plurality of tamper verification functions, that a tamper code and type information is embedded in the software in the application software section, and that the system section reads the tamper code and type from the application software and based on those values selects the corresponding tamper verification function to use to verify whether the software application has been tampered with or not with the motivation to optimize protection without imposing much burden in operation (Togawa, col. 4, lines 1-5).

5.   Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sullivan in view of

Harvey et al. (U.S. Patent 4,704,725 and Harvey hereinafter).

In regards to claim 8, Sullivan teaches the system of claim 7 as discussed above.

Sullivan does not teach wherein the information concerning said application software is

information indicating the name of said application software, or the version number of said

application software, or a tamper code, or the type of a tamper resistance verification function, or

information concerning user.

Harvey teaches a method and apparatus for automatically controlling programming

transmissions and presentations on television and radio equipment and monitoring the

programming transmitted and presented (see Abstract).

Harvey teaches wherein the embedded information concerning said application software

is information indicating the name of said application software, or the version number of said

application software, or a tamper code, or the type of a tamper resistance verification function, or

information concerning user (i.e. signal processor, 200, also passes the customer's name and

address and its own unique apparatus identifier code from read only memory, 21, to signal

generator, 230, which generates a signal embedding the customer's name and address and the

retail outlet's identification in the programming in a suitable place or places in a suitable fashion.

Signal processor, 200, may also transmit the customer's name and address to printer or other

means, 221, for actual printing of the customer's name and address in the text.) (col. 21, lines 65-

67).

Therefore it would have been obvious to one of ordinary skill in the art at the time of

Applicant's invention to modify the teaching of Sullivan with the teachings of Harvey to include

wherein the information concerning said application software is information indicating the name

of said application software, or the version number of said application software, or a tamper

code, or the type of a tamper resistance verification function, or information concerning user

with the motivation to prevent the unauthorized use of signals and programming (Harvey, col. 3,

lines 17-18).

Other Prior Art Made of Record

6.   A.   Arnold et al. (U.S. Patent No. 4,558,176) discloses computer systems to inhibit

unauthorized copying, unauthorized usage, and automated cracking of protected software;

B.   Arnold (U.S. Patent No. 5,787,172) discloses an apparatus and method for

establishing a cryptographic link between elements of a system;

C.   Alcorn et al. (U.S. Patent No. 6,149,522) discloses a method of authenticating

game data sets in an electronic casino gaming system; and

D.   Wehrenberg (U.S. Patent No. 6,523,113) discloses a method and apparatus for

copy protection.

Conclusion

7.   The prior art made of record and not relied upon is considered pertinent to applicant's
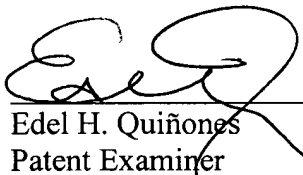
disclosure.

Points of Contact

8.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Edel H. Quiñones whose telephone number is 703-305-8745.

The examiner can normally be reached on M-F (8:00AM-5:00PM).
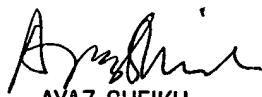
If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the

organization where this application or proceeding is assigned is 703-305-3718.

Any inquiry of a general nature or relating to the status of this application or proceeding

should be directed to the receptionist whose telephone number is 703-305-3900.

Edel H. Quiñones
Patent Examiner
Technology Center 2100

April 2, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100